REMARKS

I.   Introduction

In response to the Office Action dated December 7, 2007, which was made final, and in conjunction with the Request for Continued Examination (RCE) submitted herewith, claims 30 and 46 have been amended. Claims 1-58 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II.   Statutory Subject Matter Rejections

In paragraph (3) of the Office Action, claims 30-58 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Applicant's attorney has amended claims 30 and 46 to overcome this rejection.

However, Applicant's attorney previously amended claims 30 and 46 to overcome the rejection under 35 U.S.C. §101 in the response to the previous Office Action. At that time, Applicant's attorney requested that, should issues still remain in this regard, the Examiner indicate how the rejection can be overcome, in accordance with the directives of the Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility. See Interim Guidelines II. Specifically, Applicants' attorney requested that the Examiner identify features of the invention that would render the claimed subject matter statutory if recited in the claim. See Interim Guidelines IV.B, as well as M.P.E.P. § 2106.

In view of the change of Examiners in this application, Applicant's attorney reiterates the request that the Examiner indicate how the rejection can be overcome, should issues still remain in this regard.

III.   Prior Art Rejections

A.   The Office Action Rejections

In paragraph (4) of the Office Action, claims 1, 17, 21, 25, 30, 46, 50, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dulude et al., U.S. Patent No. 6,310,966 (Dulude) in view of Epstein, U.S. Publication No. 2002/0124176 (Epstein). In paragraph (5) of the Office Action, claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, and 55-58 were rejected under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of Epstein and further in view of Musgrave et al., U.S. Patent No. 6,202,151 (Musgrave).

Applicant's attorney respectfully traverses these rejections.

-10-

B.   Applicant's Invention

Applicant's invention, as recited in independent claims 1, 17, 30 and 46, is generally directed to processing data to enable the authorized submission and authentication of biometric data in a confidential manner. Claim 1 is representative, and recites:

receiving a first biometric data and a first personal key;

processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a first processed data;

receiving a second biometric data and a second personal key;

processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data;

eliminating all storage or trace of the first and second biometric data and personal keys in an unprocessed form;

comparing the second processed data to the first processed data, without accessing the first and second processed data in an unprocessed form, in order to enable authentication of the first and second biometric data and personal keys in a confidential manner; and

generating a signal pertaining to the comparison of the second processed data to the first processed data for use in an authentication process.

C.   The Dulude Reference

Dulude describes how biometric identification is combined with digital certificates for electronic authentication as biometric certificates. The biometric certificates are managed through the use of a biometric certificate management system. Biometric certificates may be used in any electronic transaction requiring authentication of the participants. Biometric data is pre-stored in a biometric database of the biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device. Subsequent transactions to be conducted over a network have digital signatures generated from the physical characteristics of a current user and from the electronic transaction. The electronic transaction is authenticated by comparison of hash values in the digital signature with re-created hash values. The user is authenticated by comparison against the pre-stored biometric certificates of the physical characteristics of users in the biometric database.

-11-

G&C 30571.302-US-U1

D.   The Epstein Reference

Epstein describes how the use of biometric information for authentication and access control is facilitated by the use of a token device. The token device contains an encryption of a key that is based on an authorized user's biometric information. The security system communicates with the token device to determine whether the current user of the token is the authorized user. The token device requires the presence of the biometric information from the authorized user to operate securely with the security system, using the biometric information to decrypt the aforementioned key for use in this security system. Thus, access will be granted only if the token is presented to the security system while the biometric information is presented to the token. An absence of either the token or the biometric information precludes access. In accordance with this invention, a copy of the biometric information is useless without the token, and the effects of a breach of security of both the biometric information and token can be minimized by invalidating the breached token.

E.   The Musgrave Reference

Musgrave describes a technique for combining biometric identification with digital certificates for electronic authentication called biometric certificates. The technique includes the management of biometric certificates through the use of a biometric certificate management system. Biometric certificates may be used in any electronic transaction requiring authentication of the participants. Biometric data is pre-stored in a biometric database of the biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device. Subsequent transactions to be conducted over a network have biometric certificates generated from the physical characteristics of a current user, which is then appended to the transaction, and which then authenticates the user by comparison against the pre-stored biometric data of the physical characteristics of users in the biometric database.

F.   The Applicant's Invention is Patentable Over the References

Applicant's claimed invention is patentable over the references, because the claims contain limitations not taught by the references. Specifically, Applicant's invention is designed to enable the authorized submission and authentication of biometric data in a confidential manner. In this regard, the biometric data is processed by an irreversible cryptographic algorithm causing the resulting data to be undecipherable, irreversible and undecryptable, but still capable of being used for comparison

-12-

G&C 30571.302-US-U1

purposes. Moreover, all traces of the unprocessed biometric data are eliminated from the system and storage.

The Office Action, on the other hand, asserts that Dulude and Epstein describes all the limitations of Applicant's independent claims:

> 4. Claims 1, 17, 21, 25, 30, 46, 50 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dulude et at. (US Patent No. 6,310,966) and in view Epstein (US Pub. No. 2002/0124176).
> As per claim 1, Dulude teaches:
> receiving a first biometric data and a first personal key;
> processing the first biometric data combined with the first personal key through an irreversible cryptographic algorithm to form a fist processed data [Fig. 4, col. 6 lines 1-5, col. 5 lines 52-62];
> receiving a second biometric data and a second personal key;
> processing the second biometric data combined with the second personal key through the irreversible cryptographic algorithm to form a second processed data [Fig. 5, col. 7 lines 7-14];
> comparing the second processed data to the first processed data, without accessing the fist and second processed data in an unprocessed form in order to enable authentication of first and second biometric data and personal keys in a confidential manner [Fig. 5, col. 7 lines 15-18]; and
> generating a signal pertaining to the comparison of the second processed data to the first processed data for use in an authentication process [Fig. 5, col. 7 lines 18-20].
> Epstein teaches:
> eliminating all storage or trace the first and second biometric data and personal keys in an unprocessed form [Fig. 4 paragraph 0029 lines 6-12].
> Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Epstein with Dulude, since one would have been motivated to provide biometric authentication and access security [Epstein, paragraph 0008 lines 1-3].

Applicant's attorney disagrees with this analysis.

Dulude describes, at the locations indicated above, the transmission of transaction biometric data and transaction data unchanged in the clear (or optionally encrypted) to a receiver. Dulude also describes the transmission of transaction biometric data and transaction data that has been one-way hashed into a first hash value, which is then encrypted using a private key to generate a digital signature. At a receiver, the transaction biometric data and transaction data that was transmitted unchanged in the clear (or optionally encrypted) is one-way hashed into a second hash value. Also at the receiver, the digital signature is decrypted using an associated public key, to obtain the first hash value, which is then compared to the second hash value, in order to authenticate the

-13-

G&C 30571.302-US-U1

transaction biometric data and transaction data, and ensure that it has not been modified during transmission.

However, these steps of Dulude mean that the biometric data and personal keys are used, transmitted and stored in an unprocessed form in Dulude, unlike Applicant's invention.

Epstein on the other hand, does not overcome these deficiencies of Dulude, notwithstanding the assertions by the Office Action that Epstein teaches eliminating all storage or trace the first and second biometric data and personal keys in an unprocessed form.

Epstein describes a token device that is used in conjunction with an individual's biometric information for authentication and access security. The token device stores a user's private key V that is symmetrically encrypted by function E using the user's biometric information B, i.e., E(V,B). The token device interacts with an access device using a conventional challenge-response method, wherein the access device communicates a random number R to the token device as a challenge. The token device uses the biometric information B to decrypt the user's private key V, and encrypts the random number R with the user's private key V, i.e., E(R, V). The token device then transmits the encrypted random number E(R, V) to the access device. The access device decrypts the encrypted random number E(R, V) with the user's public key U. If the decrypted result is identical to the original random number R that was communicated to the token device, a match is asserted and access is granted.

However, these steps of Epstein relate only to the comparison of encrypted random numbers, but not to the comparison of biometric data and personal keys, in a processed form, in to enable authentication the biometric data and personal keys in a confidential manner.

Moreover, the portions of Epstein cited by the Office Action merely refer to the discarding of the biometric information B and the private key V after the private key V has been decrypted using the biometric information B and after the random number R has been encrypted using the private key V. Nonetheless, during those decrypting and encrypting steps, both the biometric information B and the private key V are used in unprocessed form, unlike Applicant's invention.

Applicant's invention, on the other hand, does not allow recovery of the biometric data and personal key in its unprocessed (decrypted) form. Instead, Applicant's invention is directed to protecting the biometric data and personal key from being captured and revealed (a) while in transit to a central function for comparison; (b) while stored in a database for future use the in the comparisons; and (c) during the comparison itself by the central function. In this regard, Applicant's

-14-

G&C 30571.302-US-U1

invention eliminates all storage and traces of the biometric data and personal key after they are irreversibly encrypted.

Further, Applicant's attorney submits that Dulude and Epstein cannot be combined in the manner asserted by the Office Action. Dulude describes the transmission and authentication of transaction biometric data and transaction data between a transmitter and receiver, while Epstein refers to a challenge-response method that transmits and authenticates a random number R. Any attempt to combine the Dulude and Epstein references would render them operable and incapable of performing the tasks for which they were devised. Consequently, the Dulude and Epstein references cannot b combined to teach Applicant's claimed invention.

Musgrave fails to overcome the deficiencies of Dulude and Epstein. Recall that Musgrave was cited only against dependent claims 2-16, 18-20, 22-24, 26-29, 31-45, 47-49, 51-53, and 55-58, and only for teaching the various limitations of these dependent claims, but not the independent claims.

Thus, Applicant's attorney submits that independent claims 1, 17, 30 and 46 are patentable over Dulude, Epstein and Musgrave. Further, dependent claims 2-16, 18-29, 31-45 and 47-58 are submitted to be patentable over Dulude, Epstein and Musgrave in the same manner, because they are dependent on independent claims 1, 17, 30 and 46, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-16, 18-29, 31-45 and 47-58 recite additional novel elements not shown by Dulude, Epstein and Musgrave.

IV.   Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

G&C 30571.302-US-U1

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicant's undersigned attorney.
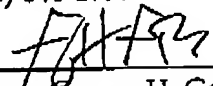
Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: <u>March 7, 2008</u>

GHG/

By:_____

Name: George H. Gates
Reg. No.: 33,500

G&C 30571.302-US-U1

-16-

G&C 30571.302-US-U1